TD 7: Coverability

Exercise 1 (Dickson's Lemma)**.** A *quasi-order* $(A, \leq)$ is a set A endowed with a reflexive and transitive ordering relation $\leq$. A *well quasi order* (wqo) is a quasi order $(A, \leq)$ s.t., for any infinite sequence $a_0 a_1 \cdots$ in A^ω, there exist indices $i < j$ with $a_i \leq a_j$.

1. Let $(A, \leq)$ be a wqo and $B \subseteq A$. Show that $(B, \leq)$ is a wqo.
2. Show that $(\mathbb{N} \uplus \{\omega\}, \leq)$ is a wqo.
3. Let $(A, \leq)$ be a wqo. Show that any infinite sequence $a_0 a_1 \cdots$ in A^ω embeds an infinite increasing subsequence $a_{i_0} \leq a_{i_1} \leq a_{i_2} \leq \cdots$ with $i_0 < i_1 < i_2 < \cdots$.
4. Let $(A, \leq_A)$ and $(B, \leq_B)$ be two wqo's. Show that the cartesian product $(A \times B, \leq_\times)$, where the product ordering is defined by $(a, b) \leq_\times (a', b')$ iff $a \leq_A a'$ and $b \leq_B b'$, is a wqo.

Exercise 2 (Coverability Graph)**.** The *coverability problem* for Petri nets is the following decision problem:

Instance: A Petri net $\mathcal{N} = \langle P, T, F, W, m_0 \rangle$ and a marking m_1 in $\mathbb{N}^P$.

Question: Does there exist m_2 in $\mathsf{reach}_\mathcal{N}(m_0)$ such that $m_1 \leq m_2$?

For 1-safe Petri nets, coverability coincides with reachability, and is thus PSpace-complete.

One way to decide the general coverability problem is to use Karp and Miller's coverability graph (see the lecture notes). Indeed, we have the equivalence between the two statements:

i. there exists m_2 in $\mathsf{reach}_\mathcal{N}(m_0)$ such that $m_1 \leq m_2$, and

ii. there exists m_3 in $\mathsf{CoverabilityGraph}_\mathcal{N}(m_0)$ such that $m_1 \leq m_3$.

1. In order to prove that (i) implies (ii), we will prove a stronger statement: for a marking m in $(\mathbb{N} \uplus \{\omega\})^P$, write $\Omega(m) = \{p \in P \mid m(p) = \omega\}$ for the set of ω-places of m.

   Show that, if $m_0 \xrightarrow{u}_\mathcal{N} m_2$ in the Petri net $\mathcal{N}$ for some u in T^*, then there exists m_3 in $(\mathbb{N} \uplus \{\omega\})^P$ such that $m_2(p) = m_3(p)$ for all p in $P \setminus \Omega(m_3)$ and $m_0 \xrightarrow{u}_G m_3$ in the coverability graph.
2. Let us prove that (ii) implies (i). The idea is that we can find reachable markings that agree with m_3 on its finite places, and that can be made arbitrarily high on its ω-places. For this, we need to identify the graph nodes where new ω values were introduced, which we call *ω-nodes.*

(a) The *threshold* $\Theta(u)$ of a transition sequence u in T^* is the minimal marking m in $\mathbb{N}^P$ s.t. u is enabled from m. Show how to compute $\Theta(u)$. Show that $\Theta(u \cdot v) \leq \Theta(u) + \Theta(v)$ for all u, v in T^*.

(b) Recall that an ω value is introduced in the coverability graph thanks to Algorithm 1.

1 **repeat**
2   *saved* $\leftarrow m'$;
3   **foreach** $m'' \in V$ *s.t.* $\exists v \in T^*, m'' \xrightarrow{v}_G m$ **do**
4   **if** $m'' < m'$ **then**
5             $m' \leftarrow m' + ((m' - m'') \cdot \omega)$
6   **end**
7   **end**
8 **until** *saved* $= m'$;
9 **return** m'

Algorithm 1: AddOmegas(m, m', V)

We consider a call to AddOmegas(m, m', V) on line 8 of the CoverabilityGraph algorithm from the course notes, where $m \xrightarrow{t}_{\mathcal{N}} m'$ for t the transition chosen at line 6 of the CoverabilityGraph algorithm.

Let $\{v_1, \ldots, v_\ell\}$ be the set of "vt" sequences, where v is found on line 3 of AddOmegas(m, m', V). These sequences vt resulted in adding at least one ω value to m' on line 5. Let $w = v_1 \cdots v_\ell$. Show that, for any k in $\mathbb{N}$, the marking ν_k defined by

$$\nu_k(p) = \begin{cases} m'(p) & \text{if } p \in P \setminus \Omega(m) \\ \Theta(w^k)(p) & \text{if } p \in \Omega(m) \end{cases}$$

allows to fire w^k. How does the marking ν'_k with $\nu_k \xrightarrow{w^k}_{\mathcal{N}} \nu'_k$ compare to ν_k?

(c) Prove that, if $m_0 \xrightarrow{u}_G m_3$ for some u in T^* in the coverability graph and m' in $\mathbb{N}^{\Omega(m_3)}$ is a partial marking on the places of $\Omega(m_3)$, then there are

- n in $\mathbb{N}$,
- a decomposition $u = u_1 u_2 \cdots u_{n+1}$ with each u_i in T^* (where the markings μ_i reached by $m_0 \xrightarrow{u_1 \cdots u_i}_G \mu_i$ for $i \leq n$ have new ω values),
- sequences $w_1, \ldots, w_n$ in T^+,
- numbers $k_1, \ldots, k_n$ in $\mathbb{N}$,

such that $m_0 \xrightarrow{u_1 w_1^{k_1} u_2 \cdots u_n w_n^{k_n} u_{n+1}}_{\mathcal{N}} m_2$ with $m_2(p) = m_3(p)$ for all p in $P \setminus \Omega(m_3)$ and $m_2(p) \geq m'(p)$ for all p in $\Omega(m_3)$.

Exercise 3 (Decidability of Model-checking Action-based LTL)**.**

1. Let $\mathcal{N}$ be Petri net, G its coverability graph, and m some marking in $\mathbb{N}^P$. An infinite *computation* is a sequence $m_0 m_1 \cdots$ in $(\mathbb{N}^P)^\omega$ where for all $i \in \mathbb{N}$, $m_i \to_{\mathcal{N}} m_{i+1}$ is a transition step. The *effect* $\Delta(u)$ of a transition sequence u in T^* is defined by $\Delta(\varepsilon) = 0^P$ and $\Delta(ut) = \Delta(u) - W(P,t) + W(t,P)$.

   Show that there exists an infinite computation s.t. $m \leq m_i$ for infinitely many indices i iff there exists an accessible loop $m' \xrightarrow{v}_G m'$ in G s.t. $m \leq m'$ and $\Delta(v) \geq 0^P$.

2. Show that action-based LTL model-checking is decidable for labeled Petri nets.

Exercise 4 (Rackoff's Algorithm)**.** A rather severe issue with the coverability graph construction is that it can generate a graph of Ackermannian size compared to that of the original Petri net. We show here a much more decent ExpSpace upper bound, which is matched by an ExpSpace hardness proof by Lipton.

Let us fix a Petri net $\mathcal{N} = \langle P, T, F, W, m_0 \rangle$. We consider *generalized markings* in $\mathbb{Z}^P$. A *generalized computation* is a sequence $\mu_1 \cdots \mu_n$ in $(\mathbb{Z}^P)^*$ such that, for all $1 \leq i < n$, there is a transition t in T with $\mu_{i+1}(p) = \mu_i(p) - W(p,t) + W(t,p)$ for all $p \in P$ (i.e. we do not enforce enabling conditions). For a subset I of P, a generalized sequence is *I-admissible* if furthermore $\mu_i(p) \geq W(p,t)$ for all p in I at each step $1 \leq i < n$. For a value B in $\mathbb{N}$, it is *I–B-bounded* if furthermore $\mu_i(p) < B$ for all p in I at each step $1 \leq i \leq n$. A generalized sequence is an *I-covering* for m_1 if $\mu_1 = m_0$ and $\mu_n(p) \geq m_1(p)$ for all p in I.

Thus a computation is a P-admissible generalized computation, and a P-admissible P-covering for m_1 answers the coverability problem.

For a Petri net $\mathcal{N} = \langle P, T, F, W, m_0 \rangle$ and a marking m_1 in $\mathbb{N}^P$, let $\ell(\mathcal{N}, m_1)$ be the length of the shortest P-admissible P-covering for m_1 in $\mathcal{N}$ if one exists, and otherwise $\ell(\mathcal{N}, m_1) = 0$. For L, k in $\mathbb{N}$, define

$$M_L(k) = \sup\{\ell(\mathcal{N}, m_1) \mid |P| = k, \max_{p \in P, t \in T} W(p,t) + \max_{p \in P} m_1(p) < L\}$$

the maximal $\ell(\mathcal{N}, m_1)$ over *all* Petri nets $\mathcal{N}$ of dimension k and all markings m_1 to cover, under some restrictions on incoming weights $W(p,t)$ in $\mathcal{N}$ and values in m_1.

1. Show that $M_L(0) \leq 1$.

2. We want to show that

   $$M_L(k) \leq (L \cdot M_L(k-1))^k + M_L(k-1)$$

   for all $k \geq 1$. To this end, we prove that, for every marking m_1 in $\mathbb{N}^P$ for a Petri net $\mathcal{N}$ with $|P| = k$,

   $$\ell(\mathcal{N}, m_1) \leq (L \cdot M_L(k-1))^k + M_L(k-1)\ . \qquad (*)$$

Let
$$B = M_L(k-1) \cdot \max_{p \in P, t \in T} W(p,t) + \max_{p \in P} m_1(p) \ .$$
and suppose that there exists a P-admissible P-covering $w = \mu_1 \cdots \mu_n$ for m_1 in $\mathcal{N}$.

(a) Show that, if w is P–B-bounded, then $(*)$ holds.

(b) Assume the contrary: we can split w as $w_1 w_2$ such that w_1 is P–B-bounded and w_2 starts with a marking μ_j with a place p such that $\mu_j(p) \geq B$. Show that $(*)$ also holds.

3. Show that $M_L(|P|) \leq L^{(3 \cdot |P|)!}$ for $L \geq 2$.

4. Given a Petri net $\mathcal{N} = \langle P, T, W, m_0 \rangle$ and a marking m_1, set $L = 2 + \max_{p \in P, t \in T} W(p,t) + \max_{p \in P} m_1(p)$. Assuming that the size n of the instance $(\mathcal{N}, m_1)$ of the coverability problem is more than
$$\max(\log L, |P|, \max_{p \in P, t \in T} \log W(t,p)) \ ,$$
deduce that we can guess a P-admissible P-covering for m_1 of length at most $2^{2^{c \cdot n \log n}}$ for some constant c. Conclude that coverability can be solved in ExpSpace.